BACKGROUND NOTE

ASEAN-India
Centre at RIS

Zone 4B, 4th floor, India Habitat Centre, Lodhi Road, New Delhi 110003
Tel: +91-11-2468 2177-80
Email: aic@ris.org.in
Website: http://aic.ris.org.in

[Version 1.0 12 January 2015. This background note has been prepared by ASEAN-India Centre at RIS to facilitate a discussion on cyber security. Usual disclaimers apply. For any further query, please contact Dr. Prabir De, Coordinator, AIC at RIS; e-mail: prabirde@ris.org.in]

Introduction

1. Cyber security covers a wide range of areas such as cyber warfare, cyber terrorism, cyber espionage, application of cyber laws, critical infrastructure protection, international cyber security cooperation, etc. In today's world, cyber security threats pose one of the most serious economic and national security challenges. Cyber security is essential for protecting information, such as personal information, financial information, sovereign data, etc. Cyber security has a global dimension and international cooperation plays an important role in strengthening cyber security capabilities.

Indian Initiatives in Cyber Security

2. India has successfully implemented a comprehensive cyber security programme in the recent past and has introduced its National Cyber Security Policy in 2013. This policy aims to facilitating secure computing environment and enabling adequate trust and confidence in electronic transactions and also guiding actions for protection of cyber space. The Information Technology (Amendment) Act, 2008 has been enacted and rules pertaining to important sections have been notified. The provisions of the Information Technology Act deal with evidentiary value of electronic transactions, digital signatures, cyber-crimes, cyber security and data protection. India has taken measures to strengthen its cyber security infrastructure, enhance awareness and upgrade skills, capabilities, and educate people to protect cyber space. India has also strengthened its cooperation in this domain with a number of friendly countries.

3. India has been collaborating with many countries for building capacity of the Law Enforcement Agencies (LEAs) in Cyber Crime Investigations and Cyber Forensics by establishing training facilities in the country. India has established world class interception capabilities for national security.

4. India has seen a massive surge in the number of cyber security incidents in the past 10 years. According to data from the Indian Computer Emergency Response Team (CERT-in), from 23 reported incidents in 2004, the number of incidents increased to 62,189 until

May 2014. For Indian companies, there has been a 20 percent increase in average losses as a consequence of security breaches, while the average cost per incident has increased to US$ 414 from US$ 194, according to a Report.[1] It has also added that employee and customer records are top targets of cyber attacks.

5. Indian Computer Emergency Response Team (CERT-in) has been operating at 24*7 basis. Steps are underway to upgrade the robust legal framework to a dynamic legal framework to enable cyber security. CERT-in has been designated under Section 70B of Information Technology (Amendment) Act 2008 to serve as the national agency to perform emergency measures for handling cyber security incidents in the country. It also issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents.

6. National Cyber Coordination Centre (NCCC) of India is a promising initiative that would help in dealing with adverse cyber activities in India.

7. Over the past years, significant efforts have been made by the National Association of Software and Services Companies (NASSCOM) to make India a secure cyber space. NASSCOM and its member organisations have launched several initiatives (through the Data Security Council of India) to promote data protection and develop security and privacy codes and standards. The group was entrusted with the task of making recommendations to the government on cyber security.

Regional Cooperation Initiatives in Cyber Security

8. The European Union's Digital Agenda sees Internet trust and security as vital to a vibrant digital society, and sets out 14 actions to improve cyber security readiness. These include establishment of a well-

[1]Refer, for example, PricewaterhouseCoopers (2015) *Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015*, available at: http://www.pwc.com/cybersecurity

functioning network of Computer Emergency Response Teams (CERTs) at national level covering all of Europe; organisation of cyber-incidents simulations and support to EU-wide cyber security preparedness. Moreover, the policy on Critical Information Infrastructure Protection (CIIP) aims to strengthen the security and resilience of vital ICT infrastructure by stimulating and supporting development of a high level of preparedness, security and resilience capabilities, both at national and at the EU level. The European Commission proposed for a Directive on Network and Information Security to put forward legal measures and give incentives to make secure cyber world.

9. In order to support member states in their fight against cyber crime, the Organization of American States (OAS), through the Inter-American Committee against Terrorism (CICTE) and the Cyber Security Program, is committed to developing and furthering the cyber security agenda in the Americas. Cooperating with a wide range of national and regional entities from the public and private sectors on both policy and technical issues, the OAS seeks to build and strengthen cyber-security capacity in the member states through technical assistance and training, policy roundtables, crisis management exercises, and the exchange of best practices related to information and communication technologies. Cyber security programme was initiated by OAS to secure cyber space for the member states. OAS introduced Inter-American Cooperation Portal on cyber-crime. This Portal was created primarily to facilitate and streamline cooperation and information exchange among government experts from OAS member states with responsibilities in the area of cybercrime or in international cooperation for its investigation and prosecution.

10. ASEAN has undertaken cyber security measures, particularly cyber confidence building measures. ASEAN Regional Forum (ARF) conducts regular Inter-Sessional Meeting on Counter Terrorism and Transnational Crime. In 2006, ARF issued Statement on Cooperation in Fighting Cyber Attack and Terrorist Misuse of Cyber Space. In 2012, ARF issued Statement on Cooperation in ensuring Cyber Security,

which aimed to intensify regional cooperation on security in the use of information and communication technologies. In 2003, ASEAN adopted the Singapore Declaration. The Declaration emphasised on the efforts to establish the ASEAN Information Infrastructure with a view to promote interoperability, interconnectivity, security and integrity. The Ministers of Telecommunications and IT decided that all ASEAN Member States develop and operationalise national Computer Emergency Response Teams (CERTs) by 2005 in line with mutually agreed minimum performance criteria. In 2011, ASEAN adopted the ASEAN ICT Master Plan 2015, in which two out of six Strategic Thrusts are relevant to the cyber dimension such as people engagement and empowerment and infrastructure development. The Master Plan on ASEAN Connectivity underlines the importance of cyber security. Under Strategy 6 of Physical Connectivity, the Master Plan recommends to (i) accelerate the development of ICT infrastructure and services in each of the ASEAN Member States, action line, (ii) to promote network integrity and information security, data protection and Computer Emergency Response Team (CERT) cooperation by developing common frameworks and establishing common minimum standards where appropriate, to ensure a level of preparedness and integrity of networks across ASEAN by 2015. ASEAN has also set-up ASEAN Network Security Action Council (ANSAC). In a meeting in 2012, held in Mactan, Cebu, ASEAN has adopted the Mactan Cebu Declaration, which has recommended continuing the collaborative activities among ASEAN Computer Emergency Response Teams (CERTs) such as the ASEAN CERTS Incident Drills (ACID), so as to enhance incident investigation and coordination amongst CERTs in support of the ASEAN Network Security Action Council (ANSAC) activities. In 2013, ARF organised a workshop on Preparedness Measures to Enhance Cyber Security – Legal and Cultural Aspects.[2]

[2] Refer, for example, ASEAN Secretariat (2014) "ASEAN's Cyber Confidence Building Measures", Presentation by the ASEAN Secretariat at UNIDIR Cyber Stability Seminar on 'Preventing Cyber Conflict', held at Geneva on 10 February 2014.

India's Initiatives with International Community in Cyber Security

11. India has taken several initiatives with global community in Cyber Security. An India-Canada bilateral meeting on ICTE was held on 6th December 2013 in New Delhi. Along with four other issues, the bilateral meeting has considered cyber security to enhance interaction between the companies/institutes from both sides. Cyber security cooperation with Japan is quite significant for India in the Asia-Pacific region. Indian Computer Emergency Response Team (CERT-in) under the Department of Electronics and Information Technology (DeitY) has signed a Memorandum of Understanding (MoU) with its counterpart Japan Computer Emergency Response Team Coordination Center (JPCERT/CC) for exchange of information and cooperation in the area of cyber security in the year 2010. With Malaysia, Indian CERT-in has shared a draft MoU on cyber security cooperation. In case of Singapore, DeitY has shown interest in promoting cooperation in cyber security, nanotechnology, mobile/cloud computing, high performance computing perception engineering, VLSI Design, 5G Wireless Networking and Electronic System Design and Manufacturing as well as in developing joint academic programmes for capacity building and human resource development. India has undertaken quite a few numbers of activities with South Korea in the area of cyber security. An MoU between CERT-In and Kr-CERT on cyber security was signed in 2014. A Joint Workshop on cyber security was held in January 2014 between CERT-In and KISA. A joint workshop for achieving mutual recognition of PKI/Digital signature was held in January 2014 between CCA and Korea Certifying Authority Central (KCAC). With the USA, an MoU between CERT-in and US-CERT was signed in 2011 to promote a closer cooperation and timely exchange of information between the organizations of their respective governments responsible for cyber security. Since, 2011 regular interactions between CERT-in and US-CERT has been taking place to share the information and discuss cyber security related issues. Besides, India has initiated IT cooperation with China, Lao PDR, Myanmar and Vietnam.

India-ASEAN Cooperation in Cyber Security: Some Recommendations

12. There are ample scopes of collaboration in the field of cyber security between ASEAN and India. ASEAN-India Plan of Action to implement the ASEAN-India partnership for peace, progress and shared prosperity (2010-2015) under the section of Economic Cooperation underlines that ASEAN and India will work on to "strengthen cooperation and capacity building in information security and cyber-security, cyber laws and regulations; joint research and development activities in the area of interactive digital media."

13. India and ASEAN should undertake initiatives to strengthen the India-ASEAN information sharing system for cyber security. Some of the ASEAN member states, particularly CLMV countries, need to strengthen its cyber security capabilities. India and ASEAN may collaborate in fostering highly-skilled human resources in the field of cyber security, including studying new measures to achieve the goal. There are scopes of collaboration in designing and implementing a competency framework for building a competent and adequate cyber security workforce.

14. There should be greater cooperation between ASEAN member states and India in combating transnational and non-traditional security challenges and specifically better coordination to deal with combating terrorism, illicit drug trafficking, human trafficking and cyber crime. India's CERT-in may explore entering an MoU with ASEAN to train human resources of ASEAN countries, particularly CLMV countries, in managing emergency measures of handling cyber security.

15. ASEAN and India may consider establishing mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts. Both should implement global security best practice and take initiative for cyber crisis management plan for all e-governance.

16. ASEAN and India can cooperate in the field of Research and Development (R&D) to protect and secure cyber space. In this regard,

CERT-in may explore the possibility of collaboration with respective national CERTs of ASEAN member states.

17. India and ASEAN shall work together to formulate initiatives to tackle emerging threats of cyber crimes, both domestically and internationally, and work forward to develop long-term cooperation on cyber security. India and ASEAN may work together to curb misuse of social media platforms in the virtual world by terror groups.

18. Efforts should be made to establish a secure business environment and secure information and communication networks as well as for enhancing the capacity for cyber security. ASEAN and India may collaborate to set up testing labs for accreditation of ICT products in order to mitigate security risks arising from procurement of ICT products especially from foreign vendors.

Objective of India-ASEAN Cyber Security Conference

19. The aim of the conference is to strengthen cooperation in the area of cyber security between India and ASEAN member states. The participants will discuss major cyber security issues confronting the ASEAN member states and India, and outline policy options to create a more resilient cyber security regime across ASEAN-India region. The conference will bring together delegates from ASEAN member states and India to exchange views on current state of technical knowledge available in cyber security and measures required to build capacity in this domain. The conference will also address national and regional cooperation efforts to promote the adoption of comprehensive and effective cyber security strategies.

20. The proceedings of the conference will help to identify the scope and opportunities for greater collaboration on cyber-related challenges between ASEAN and India, and undertake necessary policy measures to strengthen the cooperation between them.

***